International Journal of Modern Research in Engineering and Technology (IJMRET)
www.ijmret.org Volume 2 Issue 6 ǁ October 2017.

Health Information Technology Implementation Challenges and Responsive Solutions for Health Systems

Dr. Syed Adeel Ahmed & Mr. Brendan James Moore, MA

Tulane University, 800 E Commerce Rd., Elmwood, 70123, Louisiana, United States

The University of New Orleans, 2000 Lakeshore Dr., New Orleans, 70148, Louisiana, United States

Xavier University of Louisiana, 1 Drexel Drive, New Orleans, 70125, Louisiana, United States

Abstract : *Because putting patients' needs first is essential in the healthcare industries, many healthcare systems face health information technology (HIT) related challenges and a patient service dilemma.We will firstpresent the patient service dilemma and provide a high-leveloverview of technologies that have increased the productivity, efficiency in providing care, and clinical collaboration across their various healthcare campuses. Then, we will suggest changesto current HIT practice that will enableHealth Systems to be Health Insurance Portability and Accountability Act (HIPAA) compliant, while meeting the needs of patients, their expectations of care, and the changing healthcare industry.*

Keywords: HIT, Health Information Technology, IT, Health, Implementation, Business Plan, Health Systems, Information Governance, Cloud computing, Mobile technology,Wearable Technology, Electronic Health Records, Electronic Medical Records, EHR, EMR, HIPPA, Personal Health Information, PHI.

I. Introduction

Because putting patients' needs first is essential in the healthcare industries, many healthcare systems face health information technology (HIT) related challenges. We will first provide a high-level overview of technologies that have increased the productivity, efficiency in providing care, and clinical collaboration across their various healthcare campuses. Then, we will suggest changes to current HIT practice that will enable Health Systems to be Health Insurance Portability and Accountability Act (HIPAA) compliant, while meeting the needs of patients, their expectations of care, and the changing healthcare industry.

Some of the challenges that face health information technology (HIT) adoption include the following:

- Funding and the rising cost of providing healthcare services
- The time medical practitioners have to learn new systems
- The number of skilled workers and employees that are needed to manage HIT systems
- Interoperability and the fact that new HIT implementation's face integration problems with older, outdated, systems [11].

The patient service dilemma is a unique problem that arises from balancing the needs of the patients with the imperative to have efficient service.

Patient Service Dilemma: There is sometimes a tension between meeting patients needs and having an increased productivity and efficiency of service.

The cost of providing health services has increased. Drug costs and treatment costs increase, and although technology provides more methods in how to treat diseases, having the infrastructure to support such data-driven methods is another financial cost for an industry that is already facing rising costs.

Along the same line of thinking, smaller hospitals might not be able to meet security requirements that HIPAA compliance. In other words, the cost to ensure secure data governance policies are in practice might be too costly for clinics and smaller health systems.

However, having data security best practices is

important. "Some 2013 findings indicate that a little over 12% of participants had withheld information from a healthcare provider because of security concerns" [9; p. 197].

Now that patients have better access to scores of neighboring health systems, if patients feel that their data is not secure, they may shop around to other "centers of excellence" offered by other hospital systems. Patients have expectations that their data is secure, and if their data is secured, they are less likely to lie to their primary care physician, ensuring that they get appropriate healthcare treatment and improved health outcomes.

We will cover several major emerging technologies being implemented in the healthcare sector, including cloud computing, mobile technology, telemedicine, wearable technologies, and cybersecurity. We will then discuss their challenges and possible suggested changes in practices to mitigate negative outcomes in addressing the patient service dilemma.

II. Overview of HIT adoption challenges

Some of the challenges that face health information technology (HIT) adoption include the following:

- Funding and the rising cost of providing healthcare services
- The time medical practitioners have to learn new systems
- The number of skilled workers and employees that are needed to manage HIT systems
- Interoperability and the fact that new HIT implementation's face integration problems with older, outdated, systems [11].

The cost of providing health services has increased. Drug costs and treatment costs increase, and although technology provides more methods in how to treat diseases, having the infrastructure to support such data-driven methods is another financial cost for an industry that is already facing rising costs.

Along the same line of thinking, smaller hospitals might not be able to meet security requirements that HIPAA compliance. In other words, the cost to ensure secure data governance policies are in practice might be too costly for clinics and smaller health systems.

Changing an HIT policy or procedure affects many areas of an organization. Having a variety of stakeholders present when implementing HIT will ensure that all needs are being met.

The goals of HIT is to improve communication and continuity of care, reduce medical errors, standardize medical care of individuals across the health system, accelerate access to care, and protect patient's privacy through security that mitigates data breaches.

Having a wide variety of views is important to include when implementing HIT policies, procedures, and departments in a healthcare environment. All stakeholders should meet and ensure that the EHR implementation met the needs of everyone. As we have previously mentioned, theInformation Governance Reference Model (IGRM) represents a process for IG policy integration that recognizes and considers a variety of stakeholders [3]. "Although diversifying roles when making IG policy will help mitigate risk, ensuring that a diversified set of identities and stakeholders are involved is as essential" [11]. Cross-functional teams are important in forming information governance policy and incorporating a variety of views is important prior to implementing an HIT plan.

III. Cloud Computing

Many different components can be obtained via the cloud. Some use the cloud for data storage, application software, backup and recovery.

The range of services offered by Cloud services vary, and the cloud computing architecture is made up of the delivery, a network, back end platforms, and front end platforms. If you want many components to be obtained via the cloud, you can have almost everything obtained via the cloud.

In certain models, such as IaaS (Infrastructure as a Service), third-party vendors host the hardware,

software, servers, and sometimes even applications on the client's behalf.

In our office, we use a rapid development e-learning software from Ukraine called EasyGenerator, so everything is hosted through a website, and the user simply logs-on to use their cloud-computing services. The European-based service stores the data, does the cloud computing, and many things we would otherwise need to consider if we were to host those components in-house.

Another model is to only use one feature, such as taking advantage of the cloud computing power, yet storing the data locally. Or, one might only use the cloud for storage services, such as CMS (Content Management System). The components you can access via the Cloud can be determined by the business need and whether or not your approach as an information technology (IT) manager is safe, fulfills a business need, and is compliant with policies, procedures, and regulations.

Utilizing the cloud has many advantages. Using the Cloud can also help a healthcare business in many ways. First, a growing company can more easily achieve scalability. Because cloud computing use is typically pay-per-use, a small yet fast growing company can "pay as you grow."

Because third-party cloud services are in charge of their own upkeep, typically a newer company will experience higher application performance than if they attempt to keep updated on their in-house system. Also, cloud services help have a centralized, aggregated, data source, so instead of needing to store and move data across your healthcare system, everyone can simply go to the Cloud for accessing what they need.

Concerning back-up and disaster recovery, the Cloud can offer protections that paper-based Electronic Health Record (EHR) systems cannot. Patient's Personal Health Information (PHI) will not be lost in the case of a flood or natural disaster.

The Cloud's use in healthcare is needed to meet the needs of patients in a dynamic marketplace. If patients have access to the internet and resources, moving some IT EHR storage functions may allow for greater transparency between patients and their medical records. As an IT manager, think about your payor mix and your patient demographics before shifting IT functioning to a cloud-based system.

The Cloud's use in healthcare also meets the hospital's need to have health operating margins. "The global adoption for cloud services in healthcare is expected to grow from $3.73 billion in 2015 to nearly $9.5 billion by 2020" [2].

Also, if the healthcare company does not have the initial funds, using cloud-based services can allow companies to avoid upfront infrastructure costs and use their precious resources on other projects and business needs.

3.1 Challenges

One disadvantage of using the Cloud for storage or cloud computing is that typically you will be using a single vendor.

A challenging aspect of adopting cloud services is that since cloud usage is increasing, cyberattacks, such as denial of service attacks, are becoming more common. However, we can give several suggestions to management that would mitigate the negative impact those attacks would have on business operations.

3.2 Suggested Changes in Practices

First, we would suggest that when we initially assess and vet the third-party vendor we plan to use for our Cloud use, we ought to inquire what specific controls they have in place, such as what encryption they use and who has control over access keys. In this initial assessment and vetting phase, we would also ask about how often they perform a risk analysis and the results of their most recent analysis. The aim of this initial inquiry is to look for a quality third-party vendor on the front end of a purchase, since traditionally when you buy-into a Cloud vendor you may be stuck with their services for a while.

Second, since you are working through a third-party, you should have a backup plan in case of

a disaster, such as the company that has your data going out of business. Also, if you have a back-up plan, such as a locally stored back-up, your operations may not be affected in case of a denial-of-service attack. Although one of the advantages of using Cloud computing in the rapidly changing and dynamic field of healthcare is that you do not need to maintain an on premise data center resource, clinics and hospitals need to be operational in the event of an outage or denial of service.

Information technology (IT) departments can also help manage and control exponential growth of costs for cloud computing, while not being a barrier to smart use of technology. Although using cloud computing is cheaper than dealing with the initial start-up costs of having an in-house system, the cost is typically related to usage. Because of the direct relationship between cost and use when cloud computing, we have several suggestions that can help IT management control exponential growth of costs, while not being a barrier to cloud computing smart use.

First, if you are using cloud computing for storage, migrate as much static data as possible through a bulk load process and then continue to transmit incremental data.

Second, since resources can be dynamically reallocated per demand, make sure that your project is not duplicating efforts and that only those that need access to cloud computing at specific times are the ones using the system.

Before deciding to use cloud computing, assess the short-term as well as the long-term cost and keep in mind your usage. If you build an in-house infrastructure, you should ask yourself how much it will cost to keep up with improvements year-after-year. If you go with a cloud computing service, you should ask yourself about the costs of recovering from a disasters, such as if the service can no longer be provided. In a healthcare context, keeping the customer (or patient) in mind is fundamental in ensuring that your company's mission can be kept, regardless of which use of technology you choose to use.

A disadvantage of using the Cloud for storage or cloud computing is that typically you will be using a single vendor. Using a single vendor raises the question, "What if the company goes out of business?" Also, outages might occur from DoS (Denial of Service) attacks and outside threats, rather than a business closing. In case of emergencies, such as the company going out of business or a DoS attack, you should have a backup plan in place that does not require the cloud service you are considering implementing.

As a manager of an IT department, you should consider all possible scenarios when choosing to use a cloud-based decision support system. For example, if the physician cannot access decision support tool due to an internet outage, will the physician still have access to enough patient conditions and historical information to make a decent diagnosis. Also, will the patient's EHR information be backed-up on-site in the event that that the hospital cannot access the information through cloud-computing. As a manager, even though using cloud computing opens many operational advantages, ensuring you have a back-up plan is essential to making sure you can meet patients' needs in the event of an outage.

Also, HIPAA compliance is important in the medical profession. However, since cloud use is relatively new, how to meet HIPAA's standards is sometimes ambiguous, and extra effort needs to be made to ensure that you are HIPAA compliant with any cloud-based practices and personal health information (PHI) security.

In addition, you should spend extra time and effort into making sure that your cloud based service operates across department needs and technology. If you use a different system that cannot be used by others due to technologic differences within your organizations, you may have interoperability issues. Next, we will cover some advantages of the cloud.

IV. Mobile Technology

There are many reasons why mobile technology is increasing in popularity. Some of the reasons include mobile technology becoming more

affordable over time. Also, mobile technology has increased in speed, convenience, wireless connectivity, and expanded in memory, while at the same time shrinking in device size.

In addition, many mobile devices are not merely used for phone calls. Instead, mobile smart phones can access the internet and use e-mail, apps, and other functions and features that increase convenience for consumers and those providing services, such as clinicians.

Mobile technology and wearables could help us move from merely treating illness to proactively reducing the occurrence of illness. Built-in analytics and dashboards enable healthcare staff and patients to sort, filter, and drill down into the patient's health data, which can be used to proactively treat and reduce the occurrence of illness.

We will illustrate our point by pointing out the difference between "leading" and "lagging" indicators. For example, if a patient can know when they have an onset of a panic attack or heart problem by a notification of their vitals (or the "leading" indicators of a heart attack), they can proactively and more readily seek help, in-the-moment, rather than waiting for the "lagging" indicator of a heart attack (the phenomenological experiencing of a heart attack) in which case one would find out too late to do any proactive treatment.

Also, many clinics in the US use text messages to remind patients of appointments, remind patients to take medications, and to communicate lab results. With mobile technology increasing the ability for patients to have access to healthcare and other services, we do not find it surprising that mobile technology continues to increase in popularity.

4.1 Challenges

Mobile technology presents unique challenges to healthcare organizations. First, if patients demand mobile technology health support, then providing that service will incur a cost. When developing an app or website that is mobile compatible, you should consider interoperability, screen size (for user ease of access) and other technical issues.

Security is also an issue. Hackers can gain access through smart devices, which include many models of mobile phones. Healthcare organizations need to consider how devices interact with one another, and ensure that patient safety is a priority over convenience or patient satisfaction. For example, in the event of an operation that uses smart devices, making sure phones are off and best practices surrounding interference prevention should be implemented.

Also, if some of your treatments require sensors and mobile technology, then there are financial questions that need to be answers concerning whether or not the patient will bear the cost, or insurance companies, or the hospital system.

4.2 Suggested Changes in Practices

The only high-level unique to the healthcare industry mobile security advice we would give to a healthcare manager would be to be aware of how patients and providers are using mobile technologies to access sensitive information.

We would convince business management to approve spending on data security by first listing the benefits of providing data security and issues that would be avoided in addressing data security needs.

We would first cover best security practices and how they would avoid issues later down the road that would be caused by poor data security practices in every type of data security, such technical, administrative, and physical data security.

Benefits of data security include the following:

- Avoid legal and HIPAA compliance issues
- Gain patient and stakeholder trust across the health system
- Reduction of data breaches
- Gained efficiency in information handling processes.
- Gained transparency and patient access to records[11; 10].

Having good data security can also lead to financial gains for the organization, such as reimbursement for costs from the Center for

Medicare and Medicaid on safely, securely, and successfully reported HCAHPS (overall patient perception of their healthcare needs being met), CGCAHPS (clinical groups), ED CAHPS (Emergency Department) survey scores.

The HIPPA settlements for 2016 have been mostly associated with internal causes.

To help prevent external breaches, we would ensure not only that firewalls are in place, but also that internal contractors and employees are trained in safe data handling and risk mitigation practices. If employees and internal contractors are not practicing safe data handling methods for information exchange, then they may unintentionally open opportunities for external cyber breaches. For example, if documents are disposed of in flippant manners, someone may only need to go through the trash to gain access to sensitive information.

Our risk assessment procedure would include a needs analysis of current data handling practices to see if there are any gaps in what we are currently doing and what best practices dictate we should be doing.

Settlements may take 2 to 3 years to develop, and finding out a data breach occurred may be months after the breach took place, but ensuring we mitigate risk as much as possible is a necessary step in ensuring that data breaches are minimal, infrequent, and preventative measures are taken.

V. Telemedicine, Wearable Technology, and Cybersecurity

Concerning clinicians, some benefits of telemedicine are that telemedicine allows for greater communication and improved collaboration among physicians and disparate healthcare organizations. Not all clinicians are employees of hospitals, so telemedicine specialists can be hired and contribute to healthcare organizations they otherwise would not be able to assist.

Concerning patients, teleconsultations with specialists in a variety of fields allows for greater access to care. If a patient is in a rural area with no specialists or large hospitals in their immediate areas, telemedicine allows for opportunities for care that the patients might not otherwise have. Specialties include teleradiology, teledermatology, teleneurology, telepharmacy, and many other.

Having convenient access to specialty care will likely raise patient satisfaction, which will thereby increase a hospital's HCAHPS(the Hospital Consumer Assessment of Healthcare Providers and Systems) scores, which affects federal reimbursement to the hospital system. In other words, the patient, hospital system, and clinician all can benefit from telemedicine.

5.1 Challenges

With those benefits in mind, practitioners using telemedicine have to keep in mind the relatively new, and changing, laws surrounding its use and also ensure that patient's needs are actually being met, regardless of patient satisfaction scores.

Many patients are socio-economically challenged, and because of this challenge an issue is raised in healthcare. Hospitals are trying to provide the best care possible, while balancing their operational costs with the needs of the patients (cost-effective care). If a healthcare organization can send laboratory results notifications through telemedicine and make patient data available through wearables, then hospital staff and patients could save on the costs of travel, Telemedicine can also improve the bottom line of a healthcare organization, while at the same time address patients' socio-economic issue. If there is a shortage of specialists in a rural area, then telemedicine may be the fastest way to provide care, while also saving costs on the patient from traveling out of their city or state to see a specialist.

How will practicing telemedicine help the healthcare organization's bottom line? If the hospital gets federal funding based on lower readmission rates, then utilizing teleconsultation and telemedicine in preventative and after-care may increase a hospital's federal reimbursement.

5.2 Suggested Changes in Practices

Using encrypted data, while using the "Security

Rule" can help outline the boundaries of what involves reasonable and appropriate safeguards to cyberattacks. For example, if your wearable uses cloud-based computing, ensure that data is encrypted if stored through cloud services. Ensuring your Chief Technology Officer, Information Security Officer, and information and data governance policies (informed by all stakeholders) are in place is the first step in saving organizations in the healthcare field time, energy, and operating funds.

Also, even if a cloud computing provider's security is very extensive, as an IT manager in the healthcare field, you must take extra steps to ensure HIPAA compliance. Data breaches can occur in a variety of ways. Not all data breaches come from external sources and not all data breaches are intentional; however, if patient sensitive information is accessed the potential harms and misuses of the compromised data are just as costly for organizations and all parties involved.

Besides being cheaper for organizations, cloud computing may also address opportunities for improved security if implemented correctly.

- Take the opportunity to upgrade the application to the latest release.
- Deploy the application in a tightly controlled virtual network segment.
- Introduce network-level threat prevention.
- Enforce stronger controls on underlying databases.
- Eliminate all existing server-level vulnerabilities prior to cutover" [11].

Security does not come automatically by moving EHR systems to the Cloud. Malware infections, and variety of hostile and intrusive software, can compromise patient data. Besides backing-up files, ensuring you know how Cloud storage works, where the data is located, and what kinds of protections are needed for HIPAA compliance is essential to mitigating lost and mishandled sensitive patient data.

Also, be sure to outline business associate contracts for uses and disclosures of PHI (Personal Health Information), so patients are aware of the risks of losing wearables, or their PHI being accessed in unauthorized ways.

In addition, using telemedicine for specialist consultations and a value-based pay structure can allow a healthcare organization to have flexibility to changing government regulations. For example, if you use a third-party telemedicine company to outsource your specialty services and regulations change, then you will bemore easily able to adjust to shift and changing conditions than if you built an in-house support system that would need to be overhauled in the event of a regulation change.

Being flexible to changing regulations is important, and ensure that any policy or procedure put in place can be addressed in the case of a changing regulation. Using third-party telemedicine vendors is a current solution to only one aspect of HIT.

VI. Conclusion

In this paper, we have offered solutions to various recent HIT challenges facing the healthcare industry. Health systems are in a unique position compared to other companies, because of the essential need to put their customer and patients' needs first. Because of this uniqueness, a patient service dilemma is present. Emerging technologies haveincreased the productivity, efficiency in providing care, and clinical collaboration across healthcare campuses, and the balance for industry leaders and managers is to meet the needs of patients, and their expectations of care, while being adaptable to the changing healthcare industry qua business entity.

Acknowledgements

Brendan Moore is a philosopher and instructional designer currently working on a leadership development program at Ochsner Health Systems in New Orleans, Louisiana. His background includes 7+ years of university medical ethics teaching at Ohio University and several years of work in the area of information technology, instructional

technology, and applied computing systems. He studies MPS Applied Computing Systems and Technology at Tulane University, and in Engineering Management at the University of New Orleans.

Dr. Syed Adeel Ahmed is a faculty member of Division of Business at Xavier University of Louisiana and Editorial Board member/Reviewer of UJEEE at HRPUB.

REFERENCES

[1] CPS: Human Resources Consulting, 2007. "Workforce Planning Tool Kit: Environmental Scan and SWOT Analysis" cpsr.us, Workforce Planning, pp. 1-38. link
[2] Delaney, D., 2017. "Why healthcare is continuing its shift to the cloud" Health Data Management, April 27th.link
[3] EDRM.net, 2015. "IGRM IT Viewpoint" EDRM Duke Law, March 31 link
[4] Fisher, M. 2017. "Why insider breaches are on the rise," HealthData Management, June 27th.link
[5] Heizer, J.; Render, B. *Operations Management: 10th Edition*, Pearson Education Inc, 2011.
[6] (1)Goedert, J., 2017. "Decision support gives UCHealth physicians more treatment options" Health Data Management, June 8th.link
[7] (2)Goedert, J. 2017. "Insider theft compromises data of rehab center residents," HealthData Management, July 5th.link.
[8] (3)Goedert, J. 2017. "Eligibility verification snafu hits Carbondale Memorial," HealthData Management, June 28th.link.
[9] Hoyt, R.E. 2014. *Health Informatics: Practical Guide for Healthcare and Information Technology Professionals 6th edition*, Informatics Education, June.
[10] Mellen, M, 2017. "4 reasons to prioritize cloud security this year" Health Data Management, February 16th. link
[11] Moore, B. Syed, A. "Return on Investment of Diversity and Inclusion Initiatives in Information Governance" *International Journal of Modern Research in Engineering and Technology*, volume 2(1), pp. 1-9.
[12] Publicsafety.gc.ca, 2011. "Emergency Management Planning Guide 2010–2011" Canada Public Safety, Section 2-1. link
[13] Smallwood, R.F., *Information Governance: Concepts, Strategies, and Best Practices*, Wiley CIO Series, April, 2014.
[14] Terhune, Chad. "UCLA Health System data breach affects 4.5 million patients," *LA Times*, Thursday, July 17th, 2015. link.
[15] (1)Violino B., 2017. "Spending on cloud computing soars during 2016" Health Data Management, January 17th.link
[16] (2)Violino B., 2017. "Analytics initiatives are encouraging cloud adoption" Health Data Management, May 25th.link
[17] (3)Violino, B., 2017. "Majority of organizations say analytics tools fall short" Health Data Management, June 6th.link
[18] (4)Violino B., 2017. "Oracle releases Data Management Workbench Cloud Services" Health Data Management, April 27th. link